Advisory Alert

Alert Number: AAA20210301 **Date:** March 1, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	High	VLAN Unauthorized Access Vulnerability

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerabilities	VLAN Unauthorized Access Vulnerability (CVE-2021-1228)
Description	The vulnerability exists due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. A remote attacker on the local network can send a specially crafted LLDP packet and make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints.
Affected Products	Cisco Nexus 9000 Series Fabric Switches
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-unauth-access-5PWzDx2w

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.